Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 44 (2015) 413 – 422

Procedia Computer Science

2015 Conference on Systems Engineering Research

Using SysML for model-based vulnerability assessment

Soroush Bassam[a,*], Jeffrey W. Herrmann[a,b], Linda C. Schmidt[b]

[a]*Institute for Systems Research, University of Maryland, College Park, MD 20742, USA*
[b]*Department of Mechanical Engineering, University of Maryland, College Park, MD 20742, USA*

Abstract

This paper discusses the use of model-based systems engineering (MBSE) models for physical protection systems (PPS) evaluation. We discuss why MBSE methodologies can be valuable in assessment of PPS. Next, we review the steps in vulnerability assessment (VA) and describe the use of SysML models in these steps. The paper presents examples of SysML models for a VA scenario. Such models can enable the development and integration of other VA tools and reduce the time and cost of conducting VA, which will lead to safer facilities.

Peer-review under responsibility of the Stevens Institute of Technology.

Keywords: SysML; Model-Based Systems Engineering; Vulnerability Assessment; Physical Protection Systems

1. Introduction

Physical Protection Systems (PPS) are intended to protect assets and facilities. A PPS is composed of people (e.g., a response force), procedures (e.g., alarm assessment), and elements (e.g., closed-circuit television (CCTV) cameras, sensors, and locks) that contribute to protecting assets against malevolent human operations such as theft and sabotage[3]. Assets include people, information, and property. Human actions and natural occurring threats can cause serious damage and are particularly important when it comes to critical infrastructure. For instance, losing information technology (IT) infrastructure for nine or more days can bankrupt an organization[4]. Therefore, mitigating the impact of damage to a business's critical infrastructure is a high priority. Today there is heightened awareness of the possibility of damage to an organization's assets from malicious actors, domestic and foreign. From 1970 to 2010, 98,000 cases of high-profile international and domestic terrorist attacks and disrupted plots occurred[9].

* Corresponding author. Tel.: +1-301-405-4518.
E-mail address: Soroush@umd.edu

Peer-review under responsibility of the Stevens Institute of Technology.
doi:10.1016/j.procs.2015.03.025

A PPS performs three functions: detect, delay, and respond. The PPS detects a threat (e.g., an intruder) by observing and identifying it. Elements in the PPS delay the threat by increasing the time needed for it to reach its target, which provides enough time for interruption. The PPS responds by intercepting and neutralizing the threat. A state-of-the-art PPS includes sophisticated sensor systems, automated responses, and modern communication and information technology.

Vulnerability Assessment (VA) (discussed in more detail in Section 1.2) is a process for designing and evaluating a PPS. As PPS have become more complex, so have the approaches and tools available for conducting VA. Proprietary techniques and a lack of standards make sharing information between these tools difficult, however.

Model-based systems engineering (MBSE) facilitates the design and evaluation of a PPS by representing data about the facility, assets, PPS, and threats in a way that aids model-based VA approaches. Moreover, the use of a common modeling language used in systems engineering (e.g. SysML) can provide the foundation for standards and tool integration in the future.

In this paper, we review the VA process and show how the SysML models commonly used in MBSE can be used for VA. An example is used to illustrate the application of SysML models.

1.1. Model-Based Systems Engineering

INCOSE has defined MBSE as "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases[7]". When adopted, MBSE approaches result in higher productivity and less development risk compared to traditional document-based approaches[2]. Therefore, document-centered systems engineering processes will be replaced by model-based systems engineering processes[7,2]. In model-based systems engineering, a set of interconnected models are built, instantiated, and used throughout the design process[9]. These models express the structure and behavior of the system. In a structure model information about features of system components as well as relationships among them is stored. A behavior model shows various states of system components and the sequence of actions within the system. MBSE software enables the user to check these models for consistency. There are several benefits to modeling such as cost reduction and enhanced knowledge transfer[2].

The Unified Modeling Language is a general-purpose graphical modeling language that is used in various stages of software development. It provides a standard framework to generate models that describe the underlying software[5]. The Systems Modeling Language (SysML) is a specialized version of the Unified Modeling Language (UML) that exists to customize UML to better support modeling systems engineering processes[2]. SysML can be used to build models that describe a system's structure and behavior. This paper describes the use of SysML structure diagrams (e.g., block definition diagrams or BDDs) to describe a facility and its security system. We also describe behavior diagrams (e.g., activity diagrams) for modeling a threat attack scenario.

1.2. Vulnerability Assessment

Vulnerability Assessment (VA) for a facility includes three key steps: determining the PPS objectives, designing the PPS, and analyzing the PPS design[1]. In the first step, one defines the PPS objectives by characterizing the facility and describing its specifications, defining potential threats, and identifying the assets that are potential targets. In the second step, one designs a PPS by selecting and placing within the facility elements that can perform the required functions of detect, delay, and respond under scenarios likely within the set of threats. In the third step, one analyzes the PPS design to determine if it meets the objectives (that is, does it stop likely threats). If the PPS is inadequate, it should be redesigned. Otherwise, it is considered as the final PPS design.

The following sections describe how SysML models can be used in these three steps.

2. SysML Models for PPS Objectives and PPS Design

Determining the objectives for a PPS requires collecting data about the facility, its assets, and potential threats. It is crucial to properly gather, organize, and represent the collected data[1].

Facility characteristics include its physical features and its operations. Garcia[1] provided a site description form that can be used to characterize the site, including the site boundary and buildings, room locations, entry points, and existing physical protection features. Physical protection features include fences, sensors, CCTV cameras, alarm communication and display (AC&D) systems, barriers, response force availability, and the response force response time. Also required is information about the facility operations, including the major products, the processes that support these products, the work hours, emergency operations, and type and number of employees.

Threat definition is a major step in assessing the desired level of PPS effectiveness. There are various parameters that define a threat. Garcia[3] introduced a wide range of threats with different actions, motivation, and capabilities. The types of adversaries presenting threats include terrorists, criminals, and extremists. Potential actions include theft and sabotage. Adversary motivations include ideological, economic, and personal ones. A threat's capabilities can be described by the number of adversaries, their weapons and equipment, their transportation capabilities, their technical experience, and their access to insider assistance. Garcia[1] emphasized that the collected data should be organized to support prioritizing threats and evaluating PPS effectiveness.

The two primary parameters that characterize an asset are the consequence of loss and the probability of loss. These are used to establish priorities for protection that leads to PPS objectives.

For PPS design, Garcia[1] provided a data collection sheet for listing the specifications of a PPS. This data sheet includes the following sections:

- Exterior sensors, interior sensors, exterior alarm assessment, interior alarm assessment, vehicles entry control, personnel entry control, AC&D subsystem;
- Delay associated with the building or room, AC&D, equipment room, guard station, and communications hub; and
- Response and response communications.

To store the data required for these two steps SysML block definition diagrams (BDDs) can be defined and instantiated. For instance, one could create a BDD for the facility, one for the response force, one for the adversary, and one for the PPS design. (Examples of these are presented in Figures 2-4 in Section 4.)

3. SysML Models for PPS Analysis

Garcia[1] described two distinct approaches for the analysis step in VA: compliance-based and performance-based. A compliance-based approach uses checklists and a site survey to verify the presence of specified security elements. A PPS is compliant if the correct equipment is installed in the right places. A performance-based approach, on the other hand, uses information about the performance of the security elements to estimate the PPS effectiveness by evaluating a quantitative model. The criticality of the assets and the desired level of protection determine which approach is most appropriate for evaluating a PPS. A compliance-based approach is appropriate when the loss of the asset has low consequences for the stakeholders. When dealing with more valuable and critical assets, however, a performance-based approach is more appropriate.

In a performance-based approach to VA, pathway analysis is used to analyze the PPS design and determine the system effectiveness measures. Pathway analysis is used to identify the weaknesses of the system for various threat scenarios[8,1]. In pathway analysis an attack scenario is divided into several tasks that are done along the path, which starts off-site at the attacker's approach and ends at the target. Associated with each task is the task time (the time that the adversary needs to perform that task). The task time is a function of the security element characteristics and adversary's equipment.

A pathway can be displayed graphically with an adversary sequence diagram (ASD). An ASD helps an analyst identify various possible pathways and is useful in multiple pathway analysis[3]. An ASD shows the different areas along the path as well as security elements. In order to transit from one area to another an adversary has to break through or overcome a security element that connects two areas. An activity diagram can be used to represent a pathway (an example is given in Section 4).

The Estimate of Adversary Sequence Interruption (EASI) model, which was developed by Sandia National Laboratories, is a quantitative analysis tool that determines the PPS performance for a specific threat and attack scenario[1,3]. The EASI model uses performance characteristics of security elements and parts of the building structure,

including probability of detection (the probability that a security item detects the adversary) and delay (the time it takes for the adversary to pass a security element). The time required for a response force to stop an adversary is also an important factor. The EASI model can also determine a PPS's Critical Detection Point (CDP), which is the last point at which, if the PPS detects the adversary, the response force can stop the adversary before the attack is completed[8].

Optimizing the PPS design includes increasing the likelihood of detecting the adversary before the CDP and increasing the delays afterwards. So, identifying the CDP plays a key role in PPS design and optimization. There are multiple pathways that an adversary can use to reach an asset. Each pathway has its own CDP because a pathway has different security elements with different characteristics. For each pathway, one could use EASI model to determine the CDP and consequently, probability of interruption. An example of applying the EASI model is shown in Section 4. Equations 1-3 are the calculations take place within the EASI model. The output of the model is the value of the probability of interruption which is used to determine the PPS effectiveness.

Let J be the number of PPS elements along an adversary's path where timely detection can occur[8]. Let P_j^D be the probability of detection for item j, $j = 1, \ldots, J$. Let β_j^D be the non-detection probability of the component j:

$$\beta_j^D = 1 - P_j^D \tag{1}$$

Let β_D be the probability of non-detection, which is the probability that the adversary is not detected by multiple independent elements:

$$\beta_D = \prod_{j=1}^{J} \beta_j^D \tag{2}$$

The probability of interruption is the probability that the response force interrupts the attack. Let P_I be the probability of interruption:

$$P_I = 1 - \beta_D = 1 - \prod_{j=1}^{J} \left(1 - P_j^D\right) \tag{3}$$

The probability of neutralization is the probability that the security response force can successfully confront and stop the threat given they are notified timely. Let P_N be the probability of neutralization, and let P_E be the system effectiveness, which measures the level of adequacy of the PPS for a defined threat:

$$P_E = P_I \cdot P_N \tag{4}$$

A SysML parametric diagram can be used to represent the necessary parameters and these relationships. A parametric diagram enables us to integrate the detection, delay, and response capabilities of the PPS into a set of equations. The parameters used in the equations link the PPS and the facility model. The parametric model shows which components in the model affect the equations that determine PPS performance. (An example is given in Section 4).

4. Example

This section illustrates the use of SysML models for VA by considering the example of a Secure Cargo Area (SCA) facility that was presented by Garcia[1], who provided a detailed layout of the facility (Figure 1). SysML models

generated in this section are based on the information provided by Garcia. It is not the purpose of this section to verify the completeness of these information but to use SysML models to store available data.

Building description. The building is in the middle of a rectangular plot that is surrounded by the facility perimeter fence; a gate in the perimeter allows vehicles to enter the facility. The main building has a staffing area, a storage area, and a staging area. Engineers, clerks, and security managers work in rooms in the staffing area. In the storage area, cargos are stored in cages, and environmental chambers and sensitive cargos are stored in a separated controlled room. A portal connects these two areas. The storage area is connected to the staging area by a second portal through which cargo are moved. The staging area has two sections: outgoing staging and incoming staging. Cargo is moved to this area through a corridor that is connected the entrance gate. The layout of the facility is shown in Figure 1. Figure 2 is a BDD of the facility.

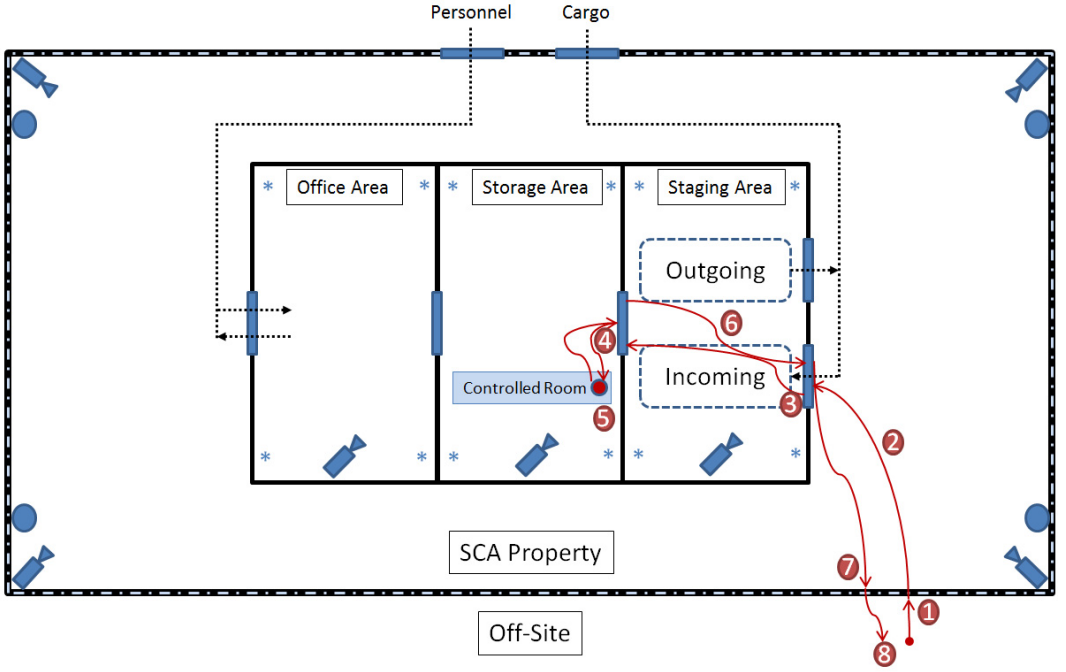


Figure 1. Layout of the SCA facility (adapted from Garcia[1])

Table 1. List of elements used in the layout of the SCA facility

Element	Icon
Fence	
Exterior Sensor	
CCTV	
Light	
Gate/Roll-Up Door	
Interior Sensor	*
Wall	
Personnel/Cargo flow	
Asset	
Adversary Path	
Adversary Task	

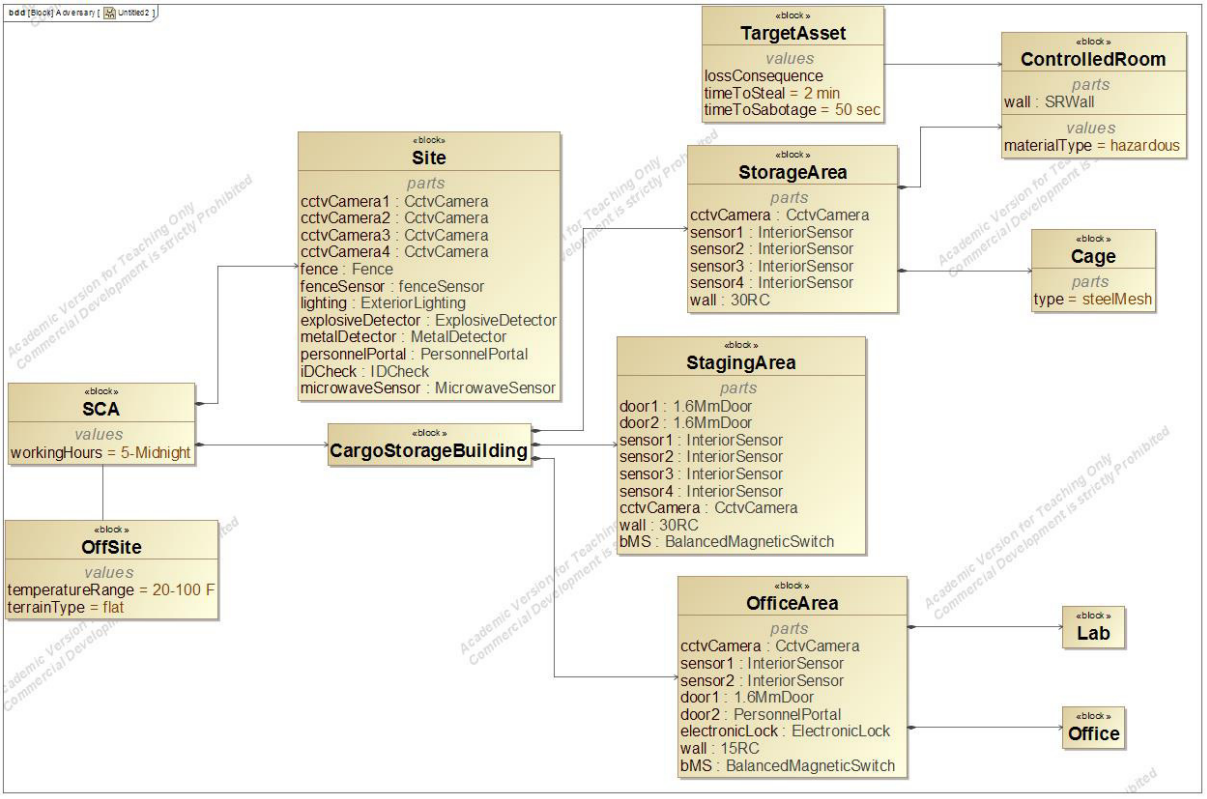
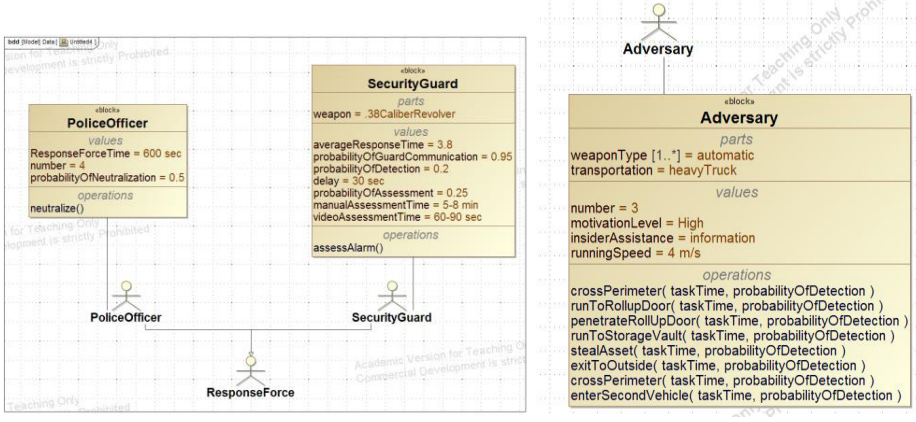


Figure 2. A BDD for the SCA facility.

PPS description. A fence located on the facility's perimeter separates the facility property from adjoining areas. There is a set of vibration sensors installed on the fence. Also, at each corner there is a fixed CCTV as well as two exterior lights to provide visibility. To further increase to detection capability at the perimeter, several microwave sensors are installed. The entrance gate is equipped with metal and explosive detectors. In the staffing area, there are two interior microwave sensors at the end of the hallway as well as a fixed CCTV.



(a) (b)

Figure 3. (a) A BDD for the response force; (b) a BDD for the adversary.

The wall of the staging area is 30-cm reinforced concrete. The wall of the staffing area is 15-cm reinforced concrete wall. The staging area and the storage area are protected by four interior microwave sensors and a CCTV. The PPS elements are shown in the Figure 1. Table 1 lists the symbols used in the figure. Figures 3(a) and 3(b) are BDDs of the response force and the adversary. Figure 4 is a BDD of the PPS design. As discussed earlier, a BDD stores the information of system components as well as relationship amongst them. As an example, the BDD shown in figure 3(a) indicates that the security guard and the police officer actors are types of the more general model for response force actor. What a security guard does is that he assesses alarms. He also has weapon which is modelled as a part property. Also, different parameters are related to the security guard such as the average response time and the assessment time and are stored in the block.

It is important to distinguish between a block, and its instances. A block is a representation of an entity and describes some of its characteristics[2]. While instances of a block have these characteristics, they may differ in the values of some characteristics. For example, in the BDD corresponding to the SCA facility, the part "cctvCamera1" in the block "Site" indicates that the CCTV Camera 1 in the site is an instance of the block "CctvCamera" in the PPS BDD diagram. In other words, there are four CCTV cameras in the site which are instances of the CCTV block in the PPS diagram. That means they share common characteristics indicated in the PPS diagram, i.e., type, color, and horizontal resolution, but they are installed in different locations.

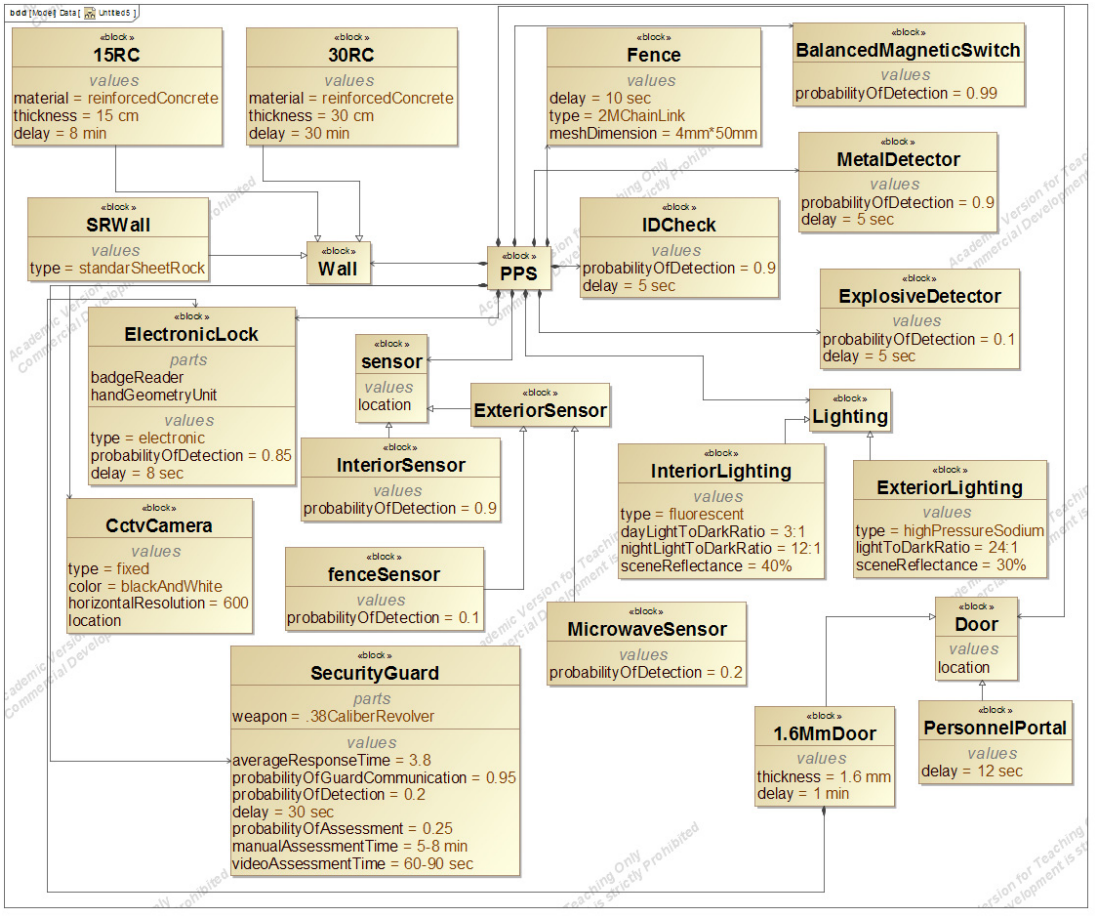


Figure 4. A BDD for the PPS design.

Attack Scenario. Three outsiders attack the facility using a large truck at night during operating hours. They are equipped with power tools and weapons. They have received information from an insider and planned their attack based on that Information. The three attackers are highly motivated, competent and able to run 4 meter/second. The target asset is located in the controlled room. Adversary tasks includes crossing the perimeter, running to the roll-up door, penetrating through the roll-up door, running to the storage vault, stealing the asset, exiting to outside, crossing the perimeter, and entering the second vehicle (Figure 1).

PPS Analysis Models. There are various pathways to the target asset. As discussed earlier, an ASD diagram provides a better understanding of different possible pathways to the target asset. Figure 5 shows various areas such as off-site, the SCA property, and the cargo storage building as well as protection layers in between them. Also, the pathway corresponding the attack scenario is shown in the figure with a dotted red line. Figure 6 is an activity diagram that shows the activities of an adversary and the response force. It stores information about the location of each adversary task, sequence of actions, and involvement of different actors.

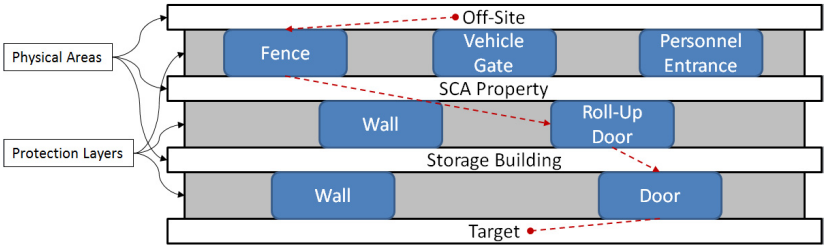


Figure 5. ASD Diagram for the example attack scenario (adapted from Garcia[1])

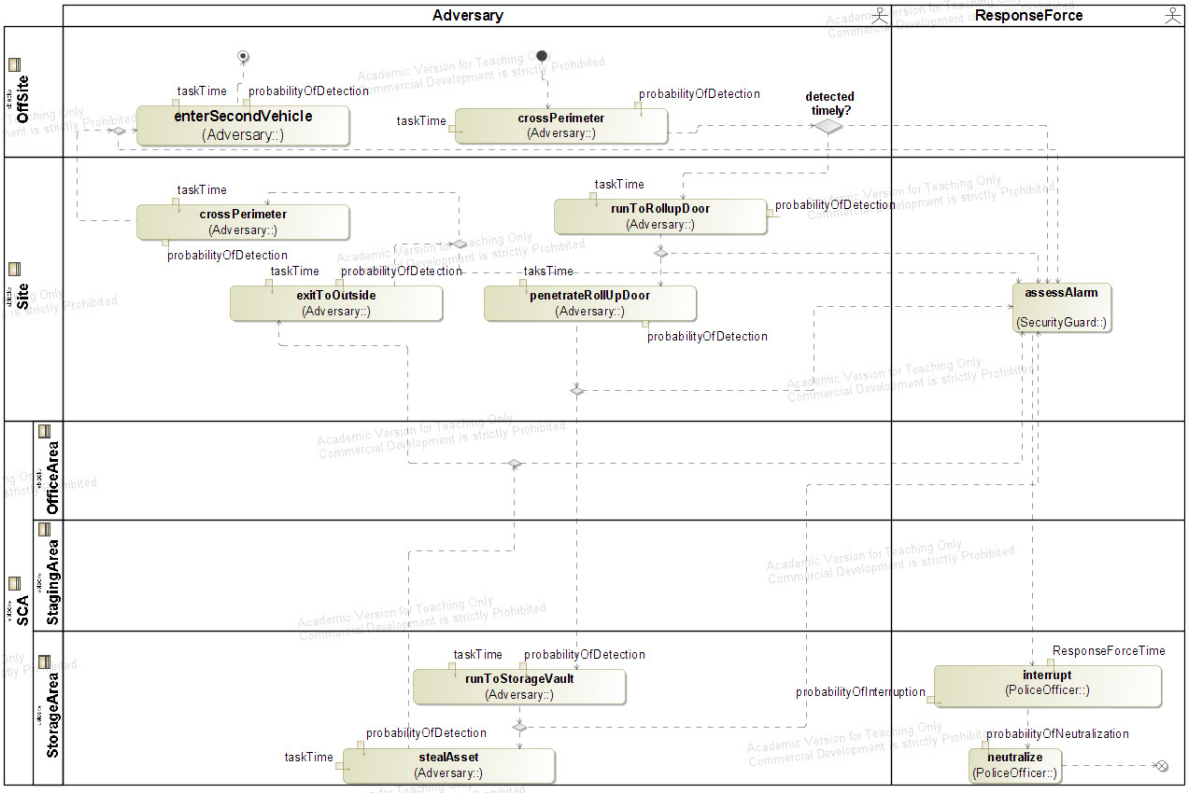


Figure 6. An activity diagram that shows the activities of an adversary and the response force.

C13 =1-(F3*F2)

	A	B	C	D	E	F
1		Adversary Task	Probability of Detection	Task Time (s)	Time Delay Remaining (s)	Non-Detection Probabilty
2	1	Cross Perimeter	0.4	30	712	0.6
3	**2**	**Run to Roll-up Door**	**0.02**	**12**	**682**	**0.98**
4	3	Penetrate Roll-up Door	0.5	120	670	
5	4	Run to Storage Vault	0.02	120	550	
6	5	Steal Asset	0.5	240	430	
7	6	Exit to outside	0.02	120	190	
8	7	Cross Perimeter	0.4	60	70	
9	8	Enter Second Vehicle	0	10	10	
10						
11		Response Force Time (s)	600			
12		Total Task Time (s)	712			
13		Probability of Interruption	0.412			
14						

Figure 7. EASI model for the example attack scenario

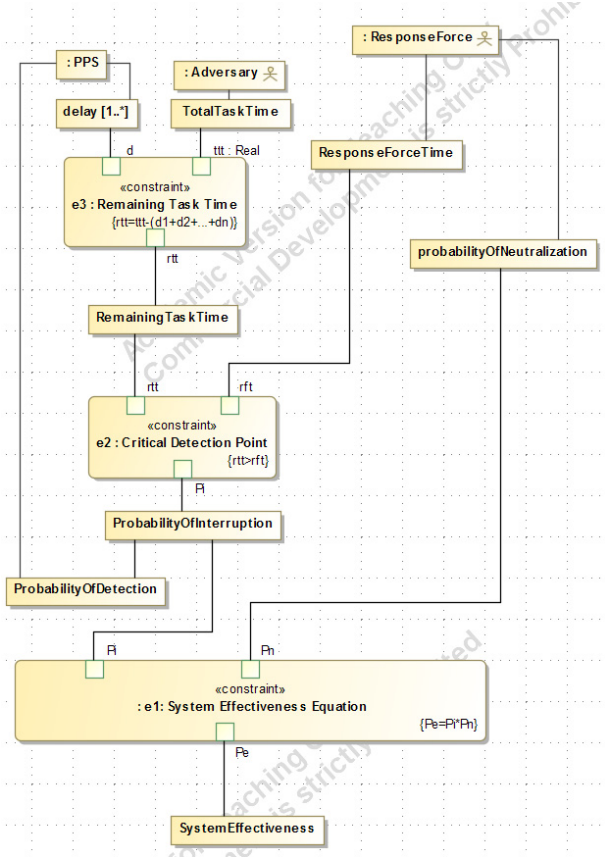


Figure 8. A parametric model for the example attack scenario

Figure 7 shows an EASI model for the attack scenario. As indicated in the figure, time it takes for the adversary to accomplish the attack after completion of task 3, is 550 seconds which is less than the RFT. Therefore, in this scenario

task 2 is the CDP, resulting in 0.412 interruption probability. Figure 8 is the corresponding parametric model for the quantitative analysis. This model shows how elements of different models affect the system effectiveness. For example, it is indicated in the figure that the RFT, a parameter in the response force model, is an input to CDP calculation.

Utilizing SysML is beneficial especially when a change occurs in the PPS because all the generated models are interconnected. Thus, when the value of a parameter in one model changes, the software automatically modifies other models with that element. For instance, if the value of probability of detection on the fence increases as a result of adding more fence sensors, the MBSE software applies adjustments to all other models that are involved (such as parametric models of different pathways that have the task "cross perimeter") .

5. Conclusion and Future Work

This paper has shown how SysML models can support PPS vulnerability assessment (VA) and thus enable model-based systems engineering (MBSE) of a PPS. The VA processes of specification, design, and analysis are essentially a system development process and thus are appropriate activities in which to use SysML models.

This paper contributes to the development of VA by demonstrating modeling techniques that can enable the development and integration of other VA tools and reduce the time and cost of conducting VA, which will lead to safer facilities.

This paper also contributes to the development of MBSE by demonstrating that its modeling approaches can be applied to other types of design and evaluation processes. The VA process is part of the larger life cycle of a facility. Although end-to-end, life-cycle use of MBSE is ideal, this paper demonstrates that, when this is not feasible, the MBSE modeling approach can be applied to a portion of the system life cycle. The implementation of separate approaches could lead eventually to ever-larger integration of developments processes using the principles of MBSE.

This paper applies MBSE principles to a particular example. We developed a series of models to facilitate the VA process. Future studies will be focused on defining a structured procedure for modeling independent of a particular case.

In the domain of VA, additional work is needed to implement robust specification, design, and analysis tools based on SysML models. The development of standards (similar to those used for building information models[6]) will further simplify VA tool development and use.

Acknowledgements

This work was sponsored by the National Institute of Standards and Technology. The views expressed in this report are those of the authors and should not be interpreted as those of the sponsor.

References

1. Garcia ML. *Vulnerability assessment of physical protection systems*. Amsterdam: Elsevier Butterworth-Heinemann; 2006.
2. Friedenthal S, Moore A, Steiner R. *A practical guide to SysML the systems modeling language*. 2nd ed. Amsterdam: Elsevier; 2012.
3. Garcia ML. *The design and evaluation of physical protection systems*. 2nd ed. Amsterdam: Elsevier Butterworth-Heinemann; 2008.
4. Baker PR, Benny DJ. *The complete guide to physical security*. Boca Raton: CRC Press; 2013.
5. Booch G, Rumbaugh J, Jacobson I. *The unified modeling language user guide*. Reading: Addison-Wesley; 1999.
6. Eastman C, Teicholz P, Sacks R, Liston K. *BIM handbook: A guide to building information modeling for owners, managers, designers, engineers, and contractors*. Hoboken: Wiley, 2008.
7. International Council on Systems Engineering. Systems Engineering Vision 2020. INCOSE-TP-2004-004-02: 2.03; 2007.
8. Physical Protection Systems. *Nuclear Safeguards Education Portal*. Available: http://nsspi.tamu.edu/nsep/courses/physical-protection-systems
9. BIPS 04 Integrated Rapid Visual Screening of Buildings. *Whole Building Design Guide*. Available: http://www.wbdg.org/ccb/DHS/bips_04.pdf